UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

UNITED STATES OF AMERICA, CRIMINAL NO. 17-134 (WMW/DTS)

Plaintiff,

v. REPORT AND RECOMMENDATION

JOHN KELSEY GAMMELL,

Defendant.

Timothy C. Rank, Assistant U.S. Attorney, 600 U.S. Courthouse, 300 South Fourth Street, Minneapolis, MN, on behalf of the Government

Rachel Paulose, Esq., DLA Piper LLP, 80 South Eighth Street, Suite 2800, Minneapolis, MN, on behalf of Defendant John Kelsey Gammell

INTRODUCTION

This case involves the prosecution of John Kelsey Gammell ("Gammell") for, among other things,[1] perpetrating repeated distributed denial of service ("DDoS") attacks on a website owned by the Washburn Computer Group. In essence, a DDoS attack will render a website in some manner inoperable or inaccessible to the public. The Government alleges Gammell's DDoS attacks on Washburn's website violated 18 U.S.C. § 1030. Gammell seeks to dismiss the Indictment, arguing that the statute under which he is being prosecuted exceeds Congress' powers under the Commerce Clause and/or is unconstitutionally vague. He also moves to suppress all evidence on

[1] On November 11, 2017, while this motion was pending, the Grand Jury returned a Superseding Indictment adding new charges, including charges of aggravated identity theft under 18 U.S.C. § 1028A, Superseding Indictment, Docket No. 46.

which the prosecution is based. The Court recommends that Gammell's motions be denied in their entirety.

FINDINGS OF FACT

This case begins with an entity called "vDOS" which provides illegal DDoS-for-hire services. Criminal Complaint ¶¶ 15, 28, Docket No. 1. DDoS-for-hire services offer their users/subscribers the ability to direct DDoS attacks against specified websites or IP addresses in exchange for a monthly subscription fee. *Id.* ¶ 15. A DDoS attack is an attempt to make a machine or network resource unavailable to its intended users, such as by interrupting or shutting down a website connected to the company or organization that is targeted. *Id.* ¶ 7. The Government alleges Gammell bought a subscription to vDOS and used it to carry out DDoS attacks against certain websites, including those of Washburn Computer Group based in Monticello, Minnesota. *Id.* ¶¶ 16, 28-41.

Washburn is a computer support, repair, and replacement provider whose website offers these products and services to the public on the internet. Def. Br. Ex. C (printouts of web pages), Docket No. 29-3. Its web pages included a phone number, a request-a-quote link to submit to Washburn, and information for customers or prospective customers about the types of equipment it will "[r]epair, [s]ell, [e]xchange and [b]uy." *Id.* The DDoS attacks on the Washburn website that are the subject of the original Indictment allegedly began on July 30, 2015. Criminal Complaint ¶ 7, Docket No. 1.

In July 2016 an internet security researcher provided a vDOS database to the Government. *Id.* ¶ 28. The database came from and was maintained by vDOS and included information from and/or about vDOS's subscribers, allegedly including

Gammell. *Id.* ¶¶ 28-29. The researcher was not directed by the Government to obtain the vDOS database nor compensated in any way for providing it. *Id.* ¶ 28.

CONCLUSIONS OF LAW

1. Motion to Suppress

A. vDOS Database

Gammell moves to suppress all evidence emanating from five subpoenas and nine search warrants issued after July 2016, which is when the internet security researcher provided the vDOS database to the Government. Def. Br. 3-4, Docket No. 27. The database contained information the Government used to obtain the subpoenas and search warrants. *Id.* at 3. Gammell contends the seized evidence is tainted fruit of the poisonous tree because the researcher was an "agent" of the Government who "improperly obtained" the vDOS database, taking "what the government knew it could not take directly." *Id.* at 2-3 (citing *Wong Sun v. United States*, 371 U.S. 471 (1963)).

A private party's actions may be attributable to the Government if the person acted as its instrument or agent under the Government's direction. *See Skinner v. Railway Labor Exec. Ass'n*, 489 U.S. 602, 613-14 (1989). However, there is no evidence in the record to support Gammell's claim that the researcher was an agent of the Government. Gammell cites to nothing except to say the researcher was "'well known' to the Government and admittedly trying to curry its favor." *Id.*; *see also* Criminal Complaint ¶ 28 ("The internet security researcher is well-known to the FBI agent to whom he provided the database, and your Affiant is also familiar with the internet security researcher's published work."), Docket No. 1. However, Gammell does

not explain why being well known to the Government makes the researcher its agent in this case. He does not allege any facts to show the researcher acted at the Government's direction. Nor does Gammell cite to anything in the record to indicate how or why the researcher was allegedly trying to "curry favor" with the Government; he does not identify where in the record it is "admitted" the researcher was trying to curry favor; and does not state how any of this makes the researcher an agent of the Government for purposes of the Fourth Amendment.

The Government states that the researcher was not directed by the Government to obtain the vDOS database and was not compensated in any way for doing so. Crim. Cmplt. ¶ 28, Docket No. 1. The Government also represented, in response to Gammell's request, that the researcher has no criminal convictions; there are no criminal acts for which charges could be brought against the researcher; and there are no plea agreements or other benefits being provided to the researcher. Gov't Br. 32, Docket No. 37. There is nothing in the record to rebut these statements.[2]

In addition, as the Government points out, Gammell has no recognized expectation of privacy in the vDOS database, including any information Gammell provided to vDOS as a subscriber to vDOS services. To establish a constitutionally cognizable privacy interest, a defendant must show (1) he has a reasonable expectation of privacy in the areas searched or the items seized, and (2) society is prepared to accept the expectation of privacy as objectively reasonable. *United States v. Wheelock*,

[2] Gammell's argument to suppress is premised upon a factual assertion for which there is no evidence in the record. Gammell asserts the internet researcher "purloined" the vDOS database by "hacking into" his or someone's computer. Def. Br. 1-2, Docket No. 27. But, as with several of Gammell's factual assertions, there is no evidence in the record to support it.

772 F.3d 825, 828 (8th Cir. 2014). The Fourth Amendment does not prohibit obtaining information that a person revealed to a third party who later conveyed that information to Government authorities, even if the person assumed that the information would be used only for a limited purpose and that the confidence placed in the third party would not be betrayed. *Id*. The information relating to Gammell's account maintained by vDOS in its database is third party information in which Gammell has no Fourth Amendment expectation of privacy. *See id.* (no expectation of privacy in subscriber information, IP address, and name obtained by the Government from an internet service provider).

Accordingly, there are no grounds to suppress the evidence obtained from warrants or subpoenas based on information from the vDOS database.

B. GPS Device

Gammell also moves to suppress the Garmin GPS device, and the information stored in and obtained from it, that the Government seized from the glove box during the search of Gammell's Buick Century. Def. Br. 4-5, Docket No. 27. Gammell contends that the search warrant for the car lacked the requisite particularity under the Fourth Amendment because it did not adequately describe the GPS device or its stored information, and the device was in the glove box, out of plain view. *Id.* at 5.

The Fourth Amendment requires that a search warrant describe particularly the place to be searched and the items to be seized. U.S. Const. Amend. IV. "To satisfy the particularity requirement of the Fourth Amendment, the items to be seized and the places to be searched must be described with sufficient particularity as to enable the searcher to locate and identify the places and items with reasonable effort and to avoid

mistakenly searching the wrong places or seizing the wrong items." *United States v. Gleich*, 397 F.3d 608, 611 (8th Cir. 2005).

The search warrant for the Buick Century authorized seizure of "all records, in whatever form, related to the 'Subject Offense'" including "any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, 'COMPUTER')." Search & Seizure Warrant, Att. B intro. ¶ and ¶ 11, Def. Br. Ex. A, Docket No. 27-1. The warrant further defines "records" and "information" to include "all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data)"; defines "computer" to include "all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions"; and defines "storage medium" to include "any physical object upon which computer data can be recorded" such as "hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media." *Id.* ¶ 11. The search warrant is not limited to only certain areas of the car. *See* Warrant, Att. A & B, Def. Br. Ex. A, Docket No. 27-1.

Gammell does not explain why the Garmin GPS device is not a "computer" or "storage device" within the scope of the warrant; instead he simply asserts that the warrant should have provided "further description of additional electronic items [the Government] wished to seize." Def. Br. 4, Docket No. 27. He seems to suggest that the warrant should have specifically said "GPS" device. *Id.* at 5.

Gammell does not dispute the Government's description of the Garmin GPS device's features and functionality in its brief (citing the company's website):

> The device performs high-speed data processing for vehicle navigation using GPS signals and up-to-date street maps that are stored on the device's memory. Users can enter in a desired address, which the device can look up in its memory and then determine the fastest route to the destination based on real-time road traffic analysis. It has a 6-inch touch-screen display, Bluetooth capabilities for calls, and voice-activated navigation. The device operates using Garmin software; contains internal memory and supports memory cards for additional data storage; logs travel history; and can transfer data to and from other computers.

Gov't Br. 36-37, Docket No. 37. This device fits within the categories and definitions in the warrant. In addition, the nature of the information stored in the GPS device – electronic data about the locations the car had visited – is expressly identified in the warrant, which states that "some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect." Affid. ¶ 48(b), Gov't Br. Ex. B, Docket No. 37-1; Warrant, Att. B intro. ¶ (incorporating affidavit), Def. Br. Ex. A, Docket No. 27-1.

The GPS device and the information stored in it fall within the scope of the search warrant for the Buick Century, and the warrant satisfies the Fourth Amendment's particularity requirement.

2. <u>Motion to Dismiss Indictment Based Upon an Unconstitutional Statute</u>

Gammell moves to dismiss the Indictment on the grounds that the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, exceeds Congress' power to regulate interstate commerce and is unconstitutionally vague. Def. Br. 1, Docket No. 29.

A. Interstate Commerce

Gammell argues that the CFAA is unconstitutional as applied to him because the Washburn Computer Group website was "not an organ of interstate commerce." *Id.* at 2, 7. A "protected computer" under the CFAA is one that "is used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B).

The Commerce Clause grants Congress the power to regulate interstate commerce. U.S. Const. Art. 1, § 8, cl. 3. "This includes the ability to regulate channels of interstate commerce, instrumentalities of interstate commerce, and those activities that substantially affect interstate commerce." *United States v. Trotter*, 478 F.3d 918, 920-21 (8th Cir. 2007) (per curiam) (citing *United States v. Lopez*, 514 U.S. 549, 558-59 (1995)). "No additional interstate nexus is required when instrumentalities or channels of interstate commerce are regulated." *Id.* at 921.

"The Internet is an international network of interconnected computers and is comparable to a sprawling mall offering goods and services." *Id.* (internal quotation marks and citations omitted). "As both the means to engage in commerce and the method by which transactions occur, the Internet is an instrumentality and channel of interstate commerce." *Id.* (internal quotation marks and citations omitted). Once a computer is used in interstate commerce, Congress has the power to protect it; the nature of the organization using the computer is irrelevant, as is the location of the attack on the computer (*i.e.*, a solely intrastate attack). *Id.* at 921-22.

Washburn's website offered products and services to the public on the internet. Def. Br. Ex. C (printouts of web pages), Docket No. 29-3. Its web pages included a phone number, a request-a-quote link to submit to Washburn, and information for

customers or prospective customers about the types of equipment it will "[r]epair, [s]ell, [e]xchange and [b]uy." *Id.* This is commercial activity. The website was "used in interstate . . . commerce or communication" and falls within the definition of a "protected computer" under the CFAA. *See* 18 U.S.C. § 1030(e)(2)(B).

Gammell does not dispute that Washburn's website was on the internet and offered products and services to the public. Rather, he contends that it was not a "protected computer" under the CFAA because the website was "very rudimentary" and "elementary;" was "basically an advertisement for services, not a channel of interstate commerce;" and allegedly had only a few visitors in the months before the DDoS attacks began. Def. Br. 2, 5-6, Docket No. 29.

Thus, Gammell seems to suggest the website is not a channel of interstate commerce because no, or very little, actual commerce was conducted on or through the site. Gammell likens the Washburn website to a billboard or a sign attached to a brick-and-mortar building, suggesting that it is a mere static advertisement rather than a channel or instrumentality of interstate commerce. *Id.* However, as *Trotter* points out, "[w]ith a connection to the Internet, … computers [are] part of a system that is inexorably intertwined with interstate commerce and thus properly within the realm of congress's commerce Clause power." *Trotter*, 478 F.3d at 921 (internal quotations and citations omitted). In short, the question is whether the website provides a channel for or is an instrumentality of interstate commerce. The constitutionality of the statute as applied to this case does not require an analysis of whether the website was an effective or well-conceived channel/instrumentality; nor does it require the Court to

determine how many people visited the website. Under *Trotter*, its very presence on the world-wide web satisfies this prong of the interstate commerce test.

Gammell also characterizes the DDoS attacks on the Washburn website as "hijinks" and "a prank;" protests that he "is no Dread Pirate Roberts," nor a "master of the cyber underworld;" and contends that the prosecution is demonstrating the sort of "federal prosecutorial indiscretion the United States Supreme Court condemned in *United States v. Lopez*, 514 U.S. 549 (1995)." *Id.* at 3, 6-7 (citing *United States v. Ulbricht*, 858 F.3d 71, 82 (2d Cir. 2017) (defendant serving life sentence for crimes including operating, under username "Dread Pirate Roberts," the Silk Road internet marketplace on which users bought and sold drugs, false identification documents, and computer hacking software)).

In essence, Gammell argues that Washburn's internet presence was too trivial, and thus the DDoS attacks were too minor to fall within Congress's regulatory power under the Commerce Clause. However, Gammell cites no authority to support the proposition that the scope of the statute is (or should be) limited to persons who "commandeer[] the web site of major commercial entities engaged in global commerce." Def. Br. 6-7, Docket No. 29. Gammell cites *Trotter* in order to contrast the attacks on the computers of a "global organization (the Salvation Army)" in that case with the "local company" (Washburn) whose website experienced DDoS attacks in this case. Def. Br. 5, Docket No. 29. However, the analysis in *Trotter* does not depend on whether the targeted organization has global or local operations; it rests on the connection to and use of the internet, which is a channel and instrumentality of interstate commerce.

The other cases cited by Gammell do not deal with the internet or any analogous channels or instrumentalities of commerce. For example, the Supreme Court in *Lopez* did not analyze Congress' authority under the Commerce Clause to regulate and protect channels and instrumentalities of commerce; rather, at issue in that case was the separate category of Congress' regulatory authority over activities that "substantially affect" interstate commerce. The court held that the Gun-Free School Zones Act exceeded Congress' authority under the Commerce Clause because the Act "neither regulates a commercial activity nor contains a requirement that the possession be connected in any way to interstate commerce." *See Lopez*, 514 U.S. at 551, 559.

Likewise, in *United States v. Morrison,* the Supreme Court again engaged in Commerce Clause analysis under the category of Congress' authority to regulate activity that "substantially affects" interstate commerce. *United States v. Morrison,* 529 U.S. 598, 609 (2000) ("Given [the statute's] focus on gender-motivated violence wherever it occurs (rather than violence directed at the instrumentalities of interstate commerce, interstate markets, or things or persons in interstate commerce), we agree that this is the proper inquiry.") The court held that Congress exceeded its authority in enacting the civil remedy provision of the Violence Against Women Act because the criminal conduct it regulated did not substantially affect interstate commerce. *Id.* at 617-18. *Morrison* did not involve channels or instrumentalities of interstate commerce. *See id.* at 618 ("The regulation and punishment of intrastate violence that is not directed at the instrumentalities, channels, or goods involved in interstate commerce has always been the province of the States.")

Other Commerce Clause cases cited by Gammell are similarly inapposite. *See Rewis v. United States,* 401 U.S. 808, 810-11 (1971) (not a federal crime to cross state lines to place a bet, or to conduct a gambling operation frequented by out-of-state bettors); *Jones v. United States*, 529 U.S. 848, 850-51 (2000) (owner-occupied private residence not used for any commercial purpose is not property "used in" commerce or commerce-affecting activity; thus, arson of that residence is not subject to prosecution under the federal arson statute).

The Court concludes that the CFAA does not violate the Commerce Clause as applied to Gammell's alleged DDoS attacks on Washburn's website.

B. Vagueness

Gammell contends that the Indictment must be dismissed because the CFAA is unconstitutionally vague. Def. Br. 7-10, Docket No. 29. Under the Fifth Amendment, a statute is void for vagueness if it (1) fails to provide a person or ordinary intelligence fair notice of what is prohibited, or (2) is so standardless that it authorizes or encourages seriously discriminatory enforcement. *United States v. Cook*, 782 F.3d 983, 987 (8th Cir. 2015). "We consider whether a statute is vague as applied to the particular facts at issue, for a [party] who engages in some conduct that is clearly proscribed cannot complain of the vagueness of the law as applied to the conduct of others." *Id.* (internal quotations and citations omitted).

Gammell does not argue that the CFAA fails to provide fair notice that a DDoS attack on a website is prohibited conduct. Rather, he claims that the statute's definition of "loss" is vague and that he "could not 'knowingly' cause $5,000 worth of damage" when the victim was unable to quantify the amount of damage right after the attack

occurred. Def. Br. 8-9, Docket No. 29. Gammell contends that the statute "carelessly defines 'loss' in a manner that essentially allows the victim to determine the defendant's level of punishment," which violates the Constitution. *Id.* at 7.

The statute defines "loss" as follows:

> (11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

18 U.S.C. § 1030(e)(11).

Gammell asserts that the "statutory definition presents more questions than answers and in no way provides a clear standard." Def. Br. 9, Docket No. 29. The Court disagrees. The plain language is clear to an ordinary person. Moreover, contrary to Gammell's assertion, this provision does not give the victim the "sole discretion . . . to determine his term of imprisonment by making the victim's loss claim a jurisdictional element of the offense." Def. Br. at 9, Docket No. 29. A jury, as instructed by the court, will ultimately decide whether the elements of the crime, including the victim's loss, have been proven.

Gammell also alleges that the Government has failed to prosecute the DDoS-for-hire entities, claiming that the "government's neglect has allowed the professional cyber hit men for hire to skip off merrily into the night." *Id.* at 10. While not entirely clear, Gammell apparently means to argue that the CFAA is therefore unconstitutionally vague because it is "so standardless that it authorizes or encourages seriously discriminatory enforcement." *See Cook*, 782 F.3d at 987. However, the only standard he complains of

is the statutory definition of "loss." *See* Def. Br. 9, Docket No. 29. As discussed above, there is nothing vague or standardless about the language that defines "loss" under the CFAA.

The language in the CFAA gave Gammell adequate notice that he could be held criminally liable for the conduct alleged in the Indictment. The statute is not unconstitutionally vague as applied to Gammell.

RECOMMENDATION

For the reasons set forth above, IT IS RECOMMENDED THAT:

1. Gammell's Motion to Suppress Seized Evidence [Docket No. 26] be DENIED; and

2. Gammell's Motion to Dismiss Indictment Based Upon an Unconstitutional Statute [Docket No. 28] be DENIED.

Dated: November 22, 2017

s/ David T. Schultz
DAVID T. SCHULTZ
United States Magistrate Judge

NOTICE

Filing Objections: This Report and Recommendation is not an order or judgment of the District Court and is therefore not appealable directly to the Eighth Circuit Court of Appeals.

Under Local Rule 72.2(b)(1), "a party may file and serve specific written objections to a magistrate judge's proposed finding and recommendations within 14 days after being served a copy" of the Report and Recommendation. A party may respond to those objections within 14 days after being served a copy of the objections. LR 72.2(b)(2). All objections and responses must comply with the word or line limits set for in LR 72.2(c).